# PCT

## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

| | | |
|---|---|---|
| (51) International Patent Classification 6 : <br><br> H04L 29/06 | A2 | (11) International Publication Number: **WO 99/56445** <br><br> (43) International Publication Date: 4 November 1999 (04.11.99) |

(21) International Application Number: PCT/SE99/00621

(22) International Filing Date: 19 April 1999 (19.04.99)

(30) Priority Data:
9801524-1     28 April 1998 (28.04.98)    SE
9802666-9     4 August 1998 (04.08.98)    SE

(71) Applicant *(for all designated States except US)*: TELIA AB (publ) [SE/SE]; Mårbackagatan 11, S-123 86 Farsta (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: HUBBARD, Elisabeth [SE/SE]; Operettvägen 28, S-142 43 Skogås (SE).

(74) Agent: PRAGSTEN, Rolf; Telia Research AB, Vitsandsgatan 9, S-123 86 Farsta (SE).

(81) Designated States: EE, LT, LV, NO, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

**Published**
*Without international search report and to be republished upon receipt of that report.*

(54) Title: A (GSM-GPRS) NETWORK WITH INTERNET PROTOCOL COMBINED FUNCTIONALITY
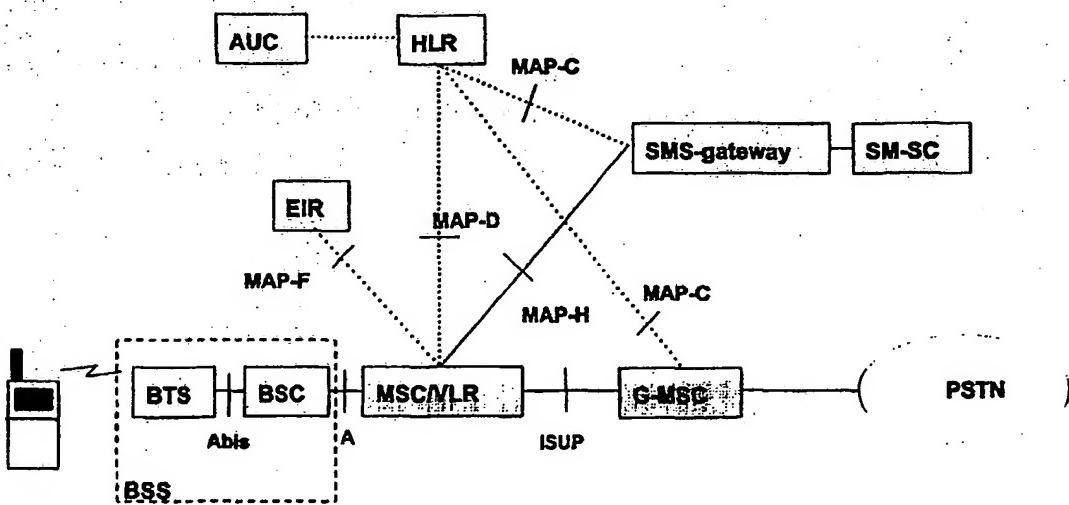
(57) Abstract

A network (GSM/GPRS) with functionality which is related to distribution of keys for authorisation, authentication and ciphering, subcriber information handling and CDR generation. The functionality is combined with the Internet protocol for transporting data and handling macro mobility to form an efficient as well as secure core network for mobile users.

A (GSM–GPRS) NETWORK WITH INTERNET PROTOCOL COMBINED FUNCTIONALITY

The present invention relates to a network (GSM/GPRS)with
functionality which is related to distribution or keys for
5    authorisation, authentication and ciphering, subscriber
information handling and CDR generation.

Since GSM (Global System for Mobile communication) was
introduced in the Nordic countries in 1992, penetration has
reached as high as 40 % – and is still increasing rapidly.
10   However, this also means that large investments have been
made in this system during those years. GSM is primarily a
system for speech communication, which makes up 98 % of the
total traffic. Data services exist, but are slow,
inefficient and expensive since they are run on circuit
15   switched connections.

In the year 2000, GSM will be enhanced with a general
packet data service (GPRS), which uses the same radio access
as GSM together with a new core network, based on IP. A
maximum of about 150 kbps can be delivered, but the actual
20   bandwidth will be significantly lower due to the presence of
other users and the quality of the radio connection.
Databases and servers containing subscriber data, equipment
data, short message handling, etc. already in operation for
the GSM system will be reused for GPRS.

25   Two years later, in 2002, UMTS (Universal Mobile
Telecommunication System) will be taken into operation,
delivering up to 2 Mbit/s over radio with full mobility.
Contrary to GPRS, the UMTS radio access network will be
built from scratch and existing core networks will be
30   modified and reused to a large extent. For the initial phase
of UMTS, the GPRS and GSM core networks are the most

interesting candidates because of their capabilities to handle mobile terminal and users.

UMTS will support mixed services, which means everything from Internet access to multimedia conferencing. Judging from how fixed Internet access presently is booming, one is tempted to believe that mobile Internet access will become equally popular. In addition, taking into account the development of IP telephony during the last year and the fact that video standards like H.323 [H.323] are being developed for IP networks, it is quite possible that an IP based network is the most future proof solution for UMTS. When constructing public mobile networks, one has to keep in mind that radio resources are scarce and that these networks are expensive to operate, and hence, it is necessary for the operator to have the means to charge the users for services that they use. In the near future, it is doubtful that this requirement can be fulfilled by (Mobile)IP networks. Operators, who have large investments in GSM and GPRS systems, could, however, reuse parts of those to complement the shortcomings of IP networks.

GSM and its future packet data service, GPRS, has an advanced system for

- authorisation and authentication of users/terminals, including key distribution
- ciphering over radio, including key distribution
- subscriber information handling
- CDR generation

through the VLR functionality in the MSC and the SGSN respectively and through the HLR and as well as other data bases.

The GPRS backbone is, however, not optimal because of its many successive protocol layers, which results in long delays and large overhead.

5    The Internet Protocol is simple, flexible and optimized for transporting data through networks. Enhanced with MobileIP for handling mobility, it could be used as a core network for mobile systems, i.e. the mobile user could get direct access to the Internet without passing through an additional

10   network, like GPRS backbone. However, IP lacks support for subscriber handling and charging. Authentication and encryption is supported to ensure integrity and confidentiality but the key distribution, which is not standardized, is still a problem. The invention offers a

15   solution of the security problem and form an efficient as well as secure core network for mobile users.

The solution to the problem is described in the claims.

20   UMTS is presently being standardardized and its core network will, in an initial phase, be based on the GPRS core network.

Advantages to the invention is that is possibly to use the fixed network in a more efficient way, when the GPRS

25   backbone, in a later stage, is replaced by a purer IP network for transporting user data under the condition that the security issues are solved.

30   Embodiments of the invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 The basic GSM architecture.

Figure 2 Overview of  the GPRS logical structure

Figure 3 The GPRS Protocol architecture. The GPRS backbone is shaded

Figure 4. General UMTS Architecture with the reference points currently identified in UMTS, March1998 [UMTS23.01].

Figure 5. Using IP for service transport end-to-end.

Figure 6. Scenario with Mobile IP support for intra UTRAN mobility and modified SGSN's to handle subscriber data etc.

Figure 7. Scenario with Mobile IP supporting roaming in foreign networks.

Figure 8. Evolution scenario for UMTS. The IWU-Gb and IWU-Gbu are taken from [umts23.20].

A glossary of the abbreviations used in this patent specification is set out below to facilitate an understanding of the present invention.

|      |                                |
|------|--------------------------------|
| AN   | Access Network                 |
| AUC  | Authentication Center          |
| BSS  | Base Sub System                |
| CN   | Core Network                   |
| DHCP | Dynamic Host Control Protocol  |

|  |  |  |
|---|---|---|
| | ETSI | European Telecommunication Standardisation Institute |
| | GGSN | Gateway GPRS Support Node |
| | GPRS | General Packet Radio Service |
| 5 | GTP | GPRS Tunneling Protocol |
| | GSM | Global System for Mobile communication |
| | HA | Home Agent |
| | HLR | Home Location Register |
| 10 | SP | Service Provider |
| | IP | Internet Protocol |
| | IWU | InterWorking Unit |
| | MS | Mobile Station |
| | MSC | Mobile Services Switching Center |
| 15 | MT | Mobile Termination |
| | PLMN | Public Land Mobile Network |
| | PSTN | Public Switched Telephone Network |
| | QoS | Quality of Service |
| | SGSN | Service GPRS Support Node |
| 20 | SIM | Subscriber Identity Module |
| | SP | Service Provider |
| | TCP | Transport Control Protocol |
| | UDP | User Datagram Protocol |
| | UE | User Equipment |
| 25 | UMTS | Universal Mobile Telecommunications System |
| | UTRAN | UMTS Terrestrial Radio Access Network |
| | VLR | Visitor Location Register |

30    UMTS, the third generation cellular system currently being
specified by ETSI, is the first cellular system to be
optimized for extensive use of data services mixed with
speech. One solution is to use the IP protocol for the

transport of services across core and access networks. Using a MobileIP core network would allow roaming between the radio access networks in a rather straightforward way. However, radio resources are scarce and public cellular

5   systems are expensive to operate, and hence, it is of great importance that the users can be properly charged for services that they use. In the near future, it is doubtful that this requirement can be fulfilled by (Mobile)IP networks. Instead, parts of GSM/GPRS could be reused to

10  complement the functionality of IP networks.

In this description, a network scenario is presented where the UMTS core network is based on Mobile IPv6, which supports roaming and possibly also handover between UTRAN's. Since the GSM/GPRS system already has several key functions

15  to handle mobile users, e.g. subscriber data, access control, keys for encryption over radio, accounting information, the GPRS SGSN node should be reused to handle the setup of lower layer communication, including authentication and check of subscriber profile etc. A

20  successful lower layer setup should be required in order to obtain a MobileIP care-of address. The mechanisms for distributing authorization and encryption keys in GSM/GPRS can also be utilized for distributing keys for the IPsec protocol.

25  Examples, describing how MobileIP and part of the GPRS core network could operate with a UMTS radio access network are presented later on in the description. The following three sections will give a brief introduction to those parts of GSM, GPRS, UMTS and IP that are relevant for this study.

30  These are followed by a short discussion on using IP end-to-end in mobile networks, before presenting the examples.

## GSM

GSM is a digital cellular system, primarily designed and
used for speech communication[gsm]. A few data services and
a rich set of supplementary services are standardized. The
5 GSM network is built up of BSS's (Base Sub System),
MSC/VLR's(Mobile Services Switching Center/Visitor Location
Register), HLR's and a few other data bases and service
nodes as illustrated in figure 1. The BSS contains base
stations and base station controllers. Each terminal is
10 equipped with a subscriber identity modules (SIM), which is
a smart card containing, among other things, the user
identity.

The MSC is the heart of the GSM system. It's duty is to:

- perform switching
15 - detect new mobile terminals in its service area
  and perform authentication and authorization
  procedures with these terminals
- collect information about users from their HLR
  and store the information in the VLR
20 - register location updates and store them in the
  VLR
- assist when handover takes place between MSC's
- create records for charging

Frequently, the VLR is integrated in the MSC. The Gateway-
25 MSC is an MSC with additional functionality to handle
traffic to and from the fixed network. For incoming traffic
the G-MSC asks the HLR for routing information to the
current MSC of the user.

The MSC communicates with databases like the home location
30 register (HLR) and the equipment identity register (EIR) via

an SS7 based signaling system called MAP (Mobile Application
Part).

The HLR stores the identity and user data of all the
subscribers belonging to the area of the related G-MSC. The
5    IMSI (International Mobile Subscriber Number), the phone
number, service profile etc. are permanently stored in the
HLR. For routing of incoming traffic, the user's current VLR
and forwarding information is stored temporarily.
Authentication and ciphering keys, which are derived in the
10   AUC (AUthentication Center) are also available from the HLR.

Authentication and authorization of the terminal takes
place each time a connection is setup, i.e. for each call.
The authentication procedure is based on the authentication
algorithm, which is stored on the SIM card and in the AUC.
15   The AUC picks a random number from which the algorithm
creates the authentication key. The random number and the
key are then passed on to the HLR and the VLR, which sends
the random number to the mobile terminal. The SIM card uses
the random number to produce the key, which is returned to
20   the network via the terminal. A comparison of the key
received from the terminal and the one originating from the
AUC will tell if the terminal is the expected one. The same
method is used for giving the terminal the encryption key,
but a different algorithm is used. This has the advantage
25   that the encryption key is never sent over radio where it
could easily be picked up by anyone. These algorithms are
known nowhere outside the home network. On the terminal
side, the algorithms are embedded in the SIM card and are
available neither to the terminal nor to the user.

30

GPRS

GPRS (General Packet Radio Service) [GSM 03.60] is a
packet switched service which, to a large extent, is based
on a combination of GSM infrastructure, IP technology and a
5  set of new functionality. Figure 2 describes the overview of
the GPRS logical architecture. The main advantage of GPRS is
that the limited radio resource is used only when there is
data to transmit. There are two kinds of support nodes in
the backbone, SGSN's (Service GPRS Support Node) and GGSN's
10  (Gateway GPRS Support Node).

The main functions of the SGSN are to:

• perform authentication and other procedures to
  let new terminals connect to its service area

• send/receive data packets to/from the GPRS mobile

15  • keep record of the mobile's location inside its
  service area

• route data packets from one GPRS operator to
  another

• produce charging data records for the charging
20  and billing system

The SGSN communicates with the HLR, the EIR, the
SMS center etc. via a GPRS version of MAP.


The main functions of the GGSN are to:

25  • route data packets from one GPRS operator to
  another

• route mobile terminated data packets to
  appropriate SGSN where the mobile is currently
  located

30  • act as a gateway between GPRS network and
  external data networks (IP, X.25, etc.)

- handle de/encapsulation of user data protocol
  packets when communicating with external data
  networks.

- produce charging data records for the charging
5    and billing system


GPRS Tunneling Protocol, GTP[gprs09.60], which is a
specific to GPRS, tunnels user data packets between SGSN's
and GGSN's. This enables the network to support transmission
10   of several packet data protocols, even if the protocol is
not supported by all SGSN's. GTP also transports signaling
data for mobility handling between the nodes. As illustrated
in figure 3, GTP is placed on top of the transport IP and
UDP layer in the protocol stack. By using a non-standard
15   protocol to transport user data, it is probably more
difficult for users to do anything harmful to the system. On
the other hand, it makes it impossible to use standard IP
tunneling mechanisms without special solutions for GTP. An
example is future resource reservation protocols, which are
20   likely to operate in combination with standard IP-in-IP
tunneling.


UMTS

The UMTS system, which currently is under specification in
25   ETSI, is based on a new UMTS Terrestrial Radio Access
Network (UTRAN) and existing, but evolved, core networks
(CN) such as IP, GSM/GPRS CN or ATM [umts23.01]. The
interworking units (IWU) adapt the different CN's to the Iu
interface if needed. The GRAN and the CN's may evolve
30   independently of each other, while the IWU's follow the
evolution of CN's and AN's to insure interconnection between
these parts. For flexibility, the user equipment consists of

different modules of which one is a UMTS version of the GSM
SIM card, the USIM. A general view of the logical modules
and reference points is shown in figure 4.

5        The UTRAN will probably have an internal mobility
management system, which means that, for routing, the CN
only needs to keep track of in which UTRAN the mobile
terminal is located. The CN will have to handle the
subscriber information management, basic call handling,
10       paging initiation, service feature analysis, security
issues, charging, etc. Evolved versions of the GSM and GPRS
CN's are foreseen for the initial phase of UMTS [umts23.20].
        Primarily, the IWU will deal with translation of protocol
messages and network parameters, in those cases where the
15       protocols in the CN and in the UTRAN are different. If the
CN does not support functionality required for a UMTS CN,
the IWU could contain intelligence to enhance the CN. The
choice of protocols over the Iu interface has not yet been
made.

20       The Internet Protocol

        The Internet Protocol, IP, is designed to route IP packets
across networks and network boundaries in a flexible and
efficient way. Because of its popularity, many services have
been developed to run on top of the IP protocol. Today, it
25       is not unusual to implement virtual IP networks within other
networks based on e.g. ATM or IP, which creates extra
security, but also additional overhead and processing time.
The GPRS backbone is one example of such a network. Taking
into account that UMTS will not be introduced until year
30       2002, we only consider IPv6 [ipv6] here.

        MobileIPv6 [mobip] is designed to deal with "macro"
mobility management, i.e. the movements of  mobile nodes

between different IP subnets. Routing in the Internet is
based on fixed IP addresses, which depends on the subnet,
through which the terminal is connected to the Internet.
When connected to a foreign network, the mobile node needs a
5      temporary address using the prefix of the visited network, a
care-of address, to be able to receive packets.

Briefly, MobileIPv6 works in the following way:

• When the mobile node arrives in a foreign subnet, it
  acquires a care-of address using the IPv6 address
10      autoconfiguration.

• The mobile node registers its care-of address with a
  router in its home subnet which acts as the node's Home
  Agent (HA). The home agent uses proxy Neighbor Discovery
  to intercept the IPv6 packets addressed to the mobile
15      node's home address. The packets are then tunneled to the
  mobile node's care-of address using IPv6 encapsulation.
  This means that the mobile node can always be addressed
  by its home address, independently of which subnet it is
  roaming in.

20  • When packets, which are tunneled from the home agent,
  arrive at the mobile node immediately sends a message,
  which includes its current care-of address, to the
  communicating node. After receiving such a packet, the
  communicating node will send packets directly to the
25      care-of address. This way, MobileIPv6 inherently supports
  optimized routing, which minimizes the load on the home
  subnet. When changing care-of address, the mobile node
  sends its new care-of address to its home agent and all
  other nodes that it is communicating with.

30

## Using IP for Service Transport Across Different Networks

Traditionally, telecom systems have been developed with one kind of transmission, for one or a few specific and well specified services which need support by the network. GSM is one example of these kind of systems where the time-to-market for new services is too long to be competitive.

UMTS should support mixed services, services provided by third-party, etc and new services must be easy and fast to implement. One possible solution is to use IP as a common format to deliver services end-to-end. This does not necessarily mean that the IP *routing* mechanisms have to be utilized in all the different networks. For example, the UTRAN has to manage micro mobility, which includes frequent and fast movements between base stations, which Mobile IP is not designed to handle. Instead, the IP layer could be provided a point-to-point connection between the IWU and the mobile terminal while the UTRAN handles the changing connections underneath.

The main advantages of this approach is that already today, an abundance of services and information is available on the Internet. Having direct Internet access from the mobile terminal would facilitate the convergence of fixed and mobile networks on a service level.

In figure 5, the end-to-end IP layer is mapped onto the UMTS architecture. The IWU would provide interworking between the lower layers of the core network and the access network.

GSM, IP and Broadband Radio Access - a Mix that
Matches

As we have seen in previous sections, the UMTS UTRAN
together with GSM/GPRS core networks would give us a system,
5    which would handle mobile users excellently and provide high
bandwidth connections over the radio interface. There is
also support for the operator to profit from running such a
network. However, neither GSM nor GPRS are designed for
large volumes and the GPRS backbone is rather inefficient
10   due to the large overhead.

On the other hand, IP is simple and flexible for
transporting data through networks. Enhanced with MobileIP,
which is optimized for roaming between subnets, it is an
interesting UMTS core network candidate. Unfortunately, it's
15   support for subscriber handling and charging is poor.

Let us therefore study how the different parts from IP,
GPRS and UMTS could interwork to support mobility. First, we
will study the case, which is illustrated in figure 6, where
20   the terminal stays within its home IP network :

• The mobile terminal arrives at a new UTRAN and listens
   to the radio broadcast messages, which contain
   information about radio parameters, network and cell
   identity, etc. as well as information about available
25   core networks, service providers, service capabilities
   etc.

• The mobile terminal sends a registration
   request including parameters such as identity,
   desired service provider etc.

30   • The UTRAN forwards the registration request to
   the SGSN, which processes it:

- The SGSN contacts the HLR of the mobile terminal
  to collect data to perform an authentication
  procedure.

- Once the terminal is authenticated and found to be
  allowed in the present UTRAN, all information over
  the radio interface can be encrypted. Encryption
  keys are obtained from the HLR. A random number is
  sent to the mobile which can calculate the key
  with an algorithm stored in the terminal. This
  way, the key is not sent over the radio interface.

- At this point, the terminal also gets
  registered in the UTRAN along with location
  data and radio specific information.

- Now, the terminal can start communicating over the IP
  layer. The terminal listens to router advertisement
  messages and solicit the nearest DHCP server [dhcp] to
  obtain a configuration parameters and a care-of-
  address. It is assumed that only stateful address
  configuration will be used, since it gives a better
  support for registration of the terminals than
  stateless. Logically, we include the IP functionality
  in the SGSN and call the entire unit SGSN' and the HLR
  records include the care-of address of the mobile
  terminal.

- The mobile terminal will then contact its home
  agent  to register its new care-of address
  according to standard MobileIP.

- The home agent has to accept or reject the registration
  of a care-of address. Before making a decision, the
  home agent could contact the HLR (via a new interface)
  to obtain information that this terminal is properly
  registered. In addition, the keys needed for using the

IPsec authentication header and/or the encapsulation
security payload [ipsec] could be obtained from the
HLR. The mobile terminal can derive its keys from
information on its USIM in the same way as in the GSM
5      system.

• While the terminal is connected and transmits data,
charging data records are produced by the SGSN'.
Systems for billing and customer handling, already in
operation for GSM, can easily be used also for UMTS.
10

In figure 7, the mobile terminal is roaming in a foreign
network. The procedure for registering in that network is
very similar to the home network case, the only difference
being that the visited SGSN' contacts the HLR in the
15     terminal's home network, either via the international SS7
network or by tunneling the MAP protocol messages through
the Internet. The mobile terminal registers with the same
home agent as before.


20     The ETSI group SMG12 works with UMTS architecture and
evolution scenarios [umts23.30]. One idea for evolution is
depicted in figure 8. The most straightforward way to
implement UMTS with an already existing GPRS network is to
attach the UTRAN to the Gb interface via the IWU-Gb.
25     However, if the UTRAN will be based on IP, a new IP based
interface, Gbu, should be opened up at the SGSN, requiring
an IWU-Gbu. In this description we have gone one step
further and transformed the SGSN into an IWU for a core
network based directly on standard IP and MobileIP.

30

UMTS, the third generation cellular system which is
currently being specified by ETSI, is the first one to be
optimized for extensive use of data services mixed with
speech. One solution is to use the IP protocol for the
5    transport of services across core and access networks. Using
a MobileIP core network would allow roaming between URAN's
in a rather straightforward way. However, radio resources
are scarce and public cellular systems are expensive to
operate, and hence, it is of great importance that the users
10   can be properly charged for the services they are using. In
the near future, it is doubtful that this requirement can be
fulfilled by (Mobile)IP networks. Instead, parts from
GSM/GPRS could be reused to complement the functionality of
IP networks.

15       In this description, a network scenario is presented where
the UMTS core network is based on Mobile IPv6, which
supports roaming and possibly also handover between UTRAN's.
Since the GSM/GPRS system already has several key functions
to handle mobile users, e.g. subscriber data, access
20   control, keys for encryption over radio, accounting
information, the GPRS SGSN node should be reused to handle
the setup of lower layer communication, including
authentication and check of subscriber profile etc. A
successful lower layer setup should be required in order to
25   obtain a MobileIP care-of address. The mechanisms for
distributing authorization and encryption keys in GSM/GPRS
can also be utilized for distributing keys for the IPsec
protocol.


30

CLAIMS

5  1       A network (GSM/GPRS)with functionality which is
related to distribution or keys for authorisation,
authentication and ciphering, subscriber information handling
and CDR generation characterised in that the functionality is
combined with the internet protocol for transporting data and
10 handling macro mobility to form an efficient as well as
secure core network for mobile users.

   2       A network, as claimed in claim 1, characterised in
that parts from GSM/GPRS is reused to complement the
15 functionality of IP networks.

   3       A network, as claimed in claim 2, characterised in
that the GPRS - SGSN is reused to handle the setup of lower
layer communication.
20

FIGURE 1

FIGURE 2

FIGURE 3

GSM / UMTS CN

N-ISDN / UMTS CN

B-ISDN / UMTS CN

PDN / UMTS CN

Au/Gbu

Nu

Bu

Pu

IWU$_1$

IWU$_2$

IWU$_3$

IWU$_4$

Iu

UTRAN

Uu

TE

TA

MT

Mobile Station

Cu

USIM
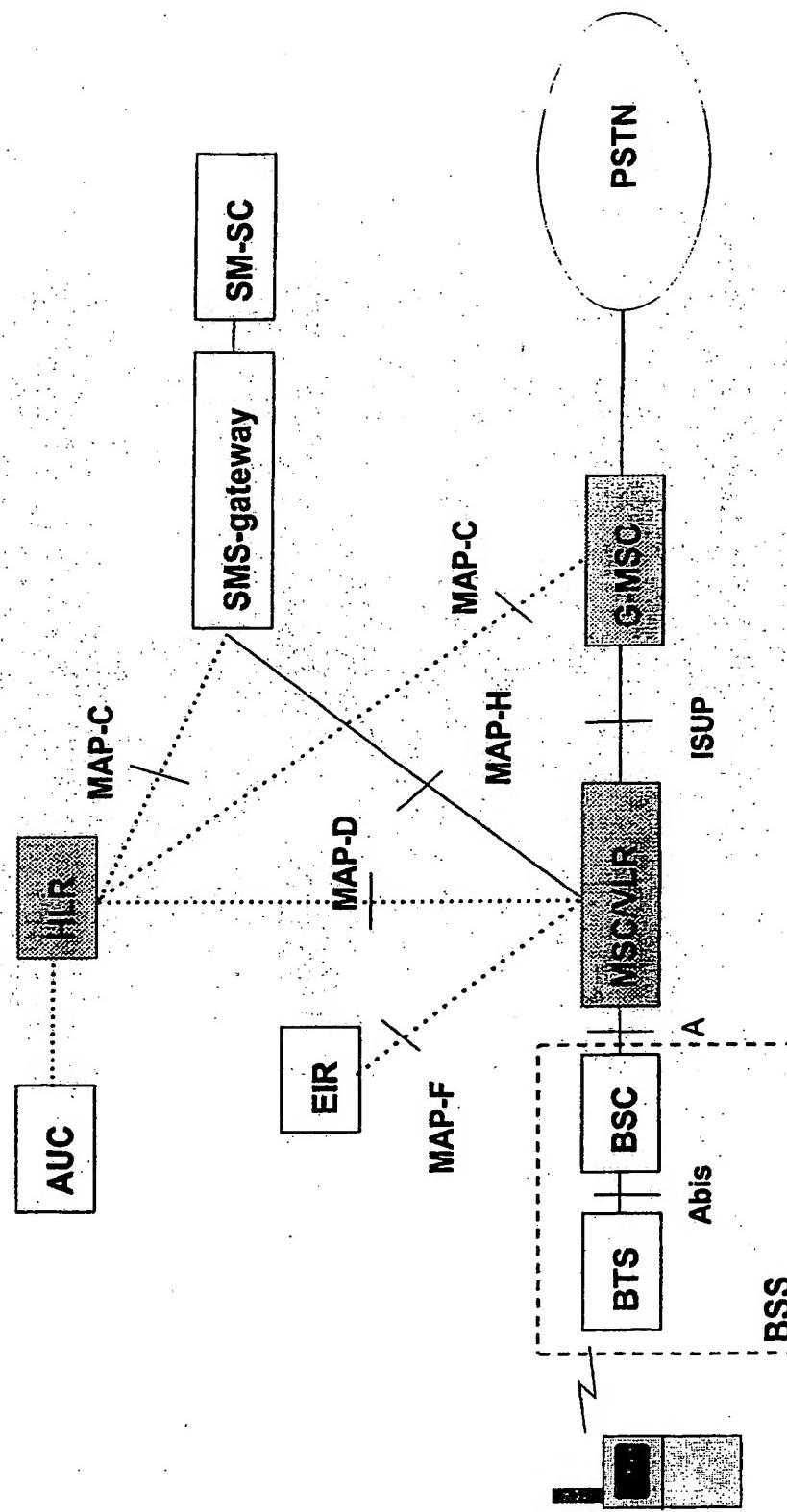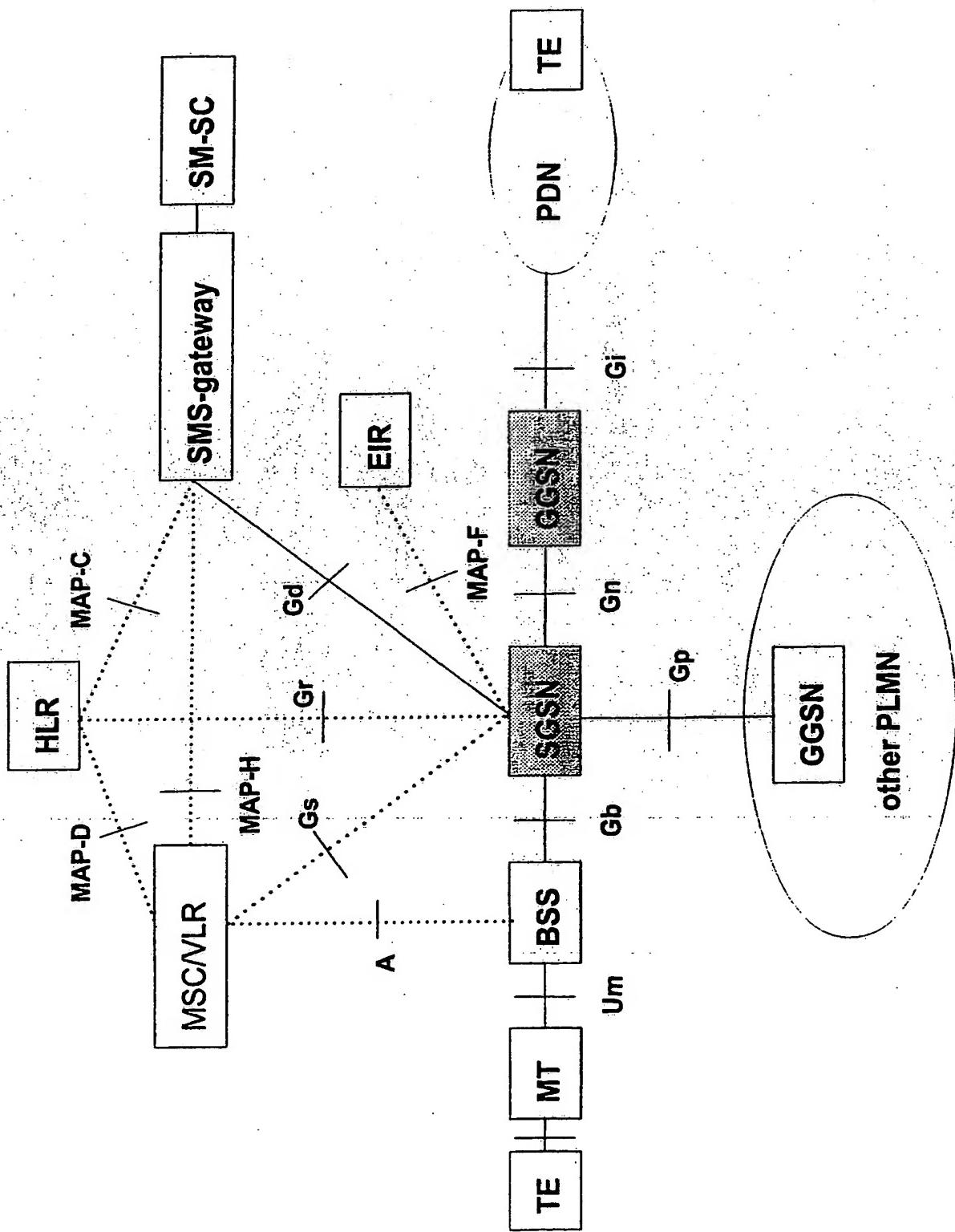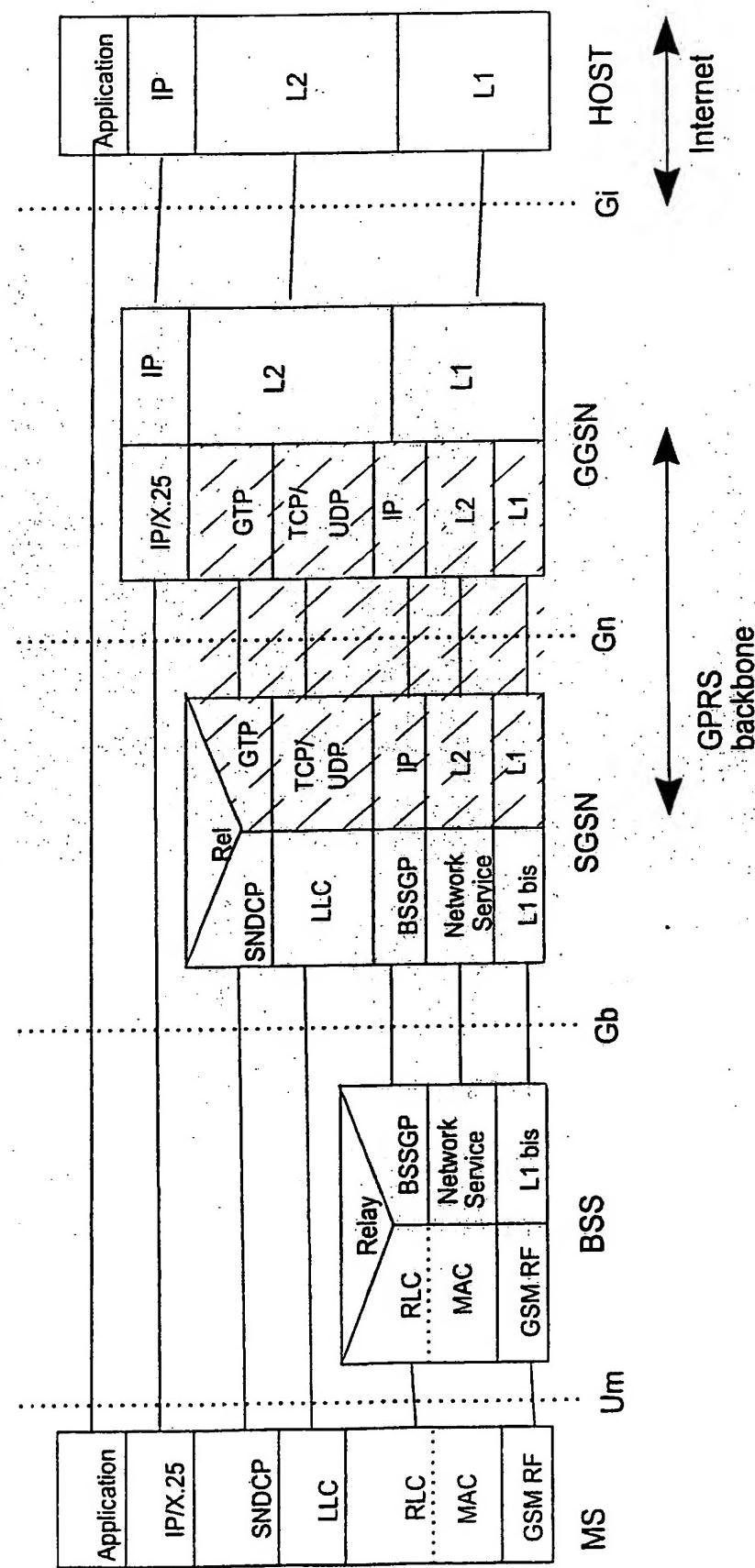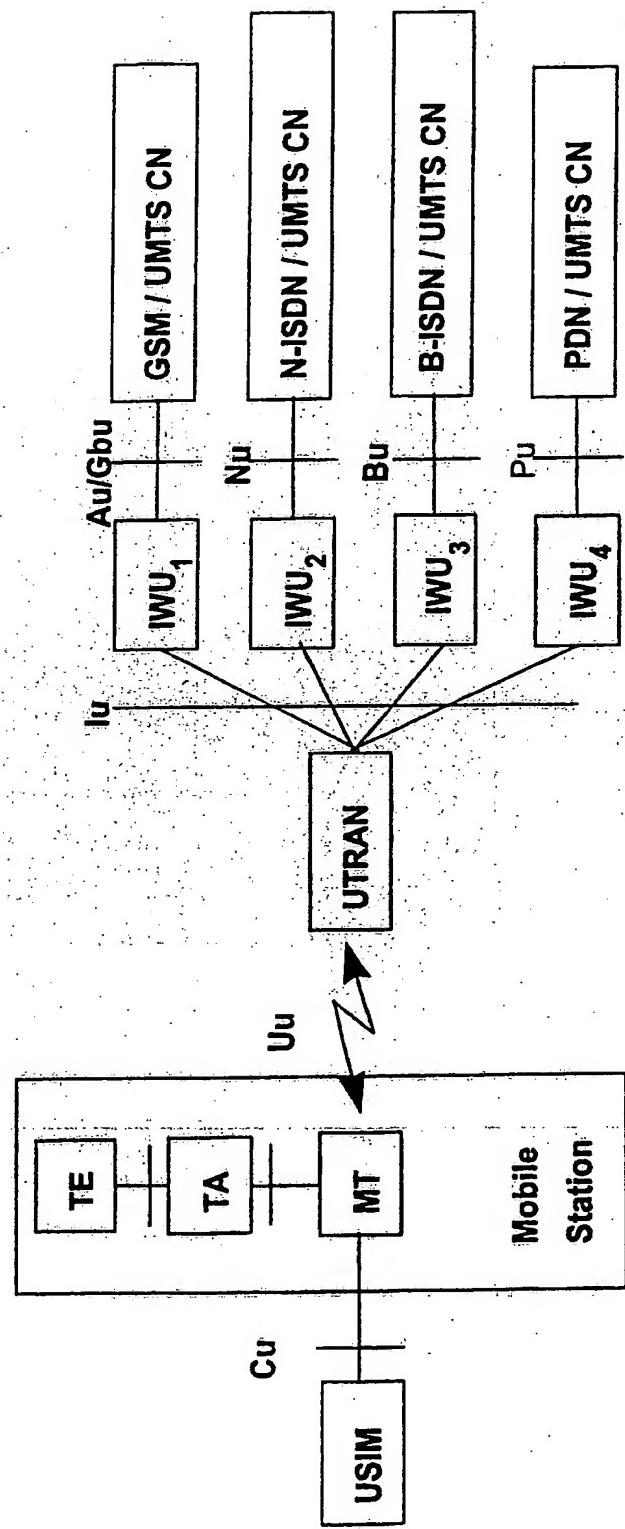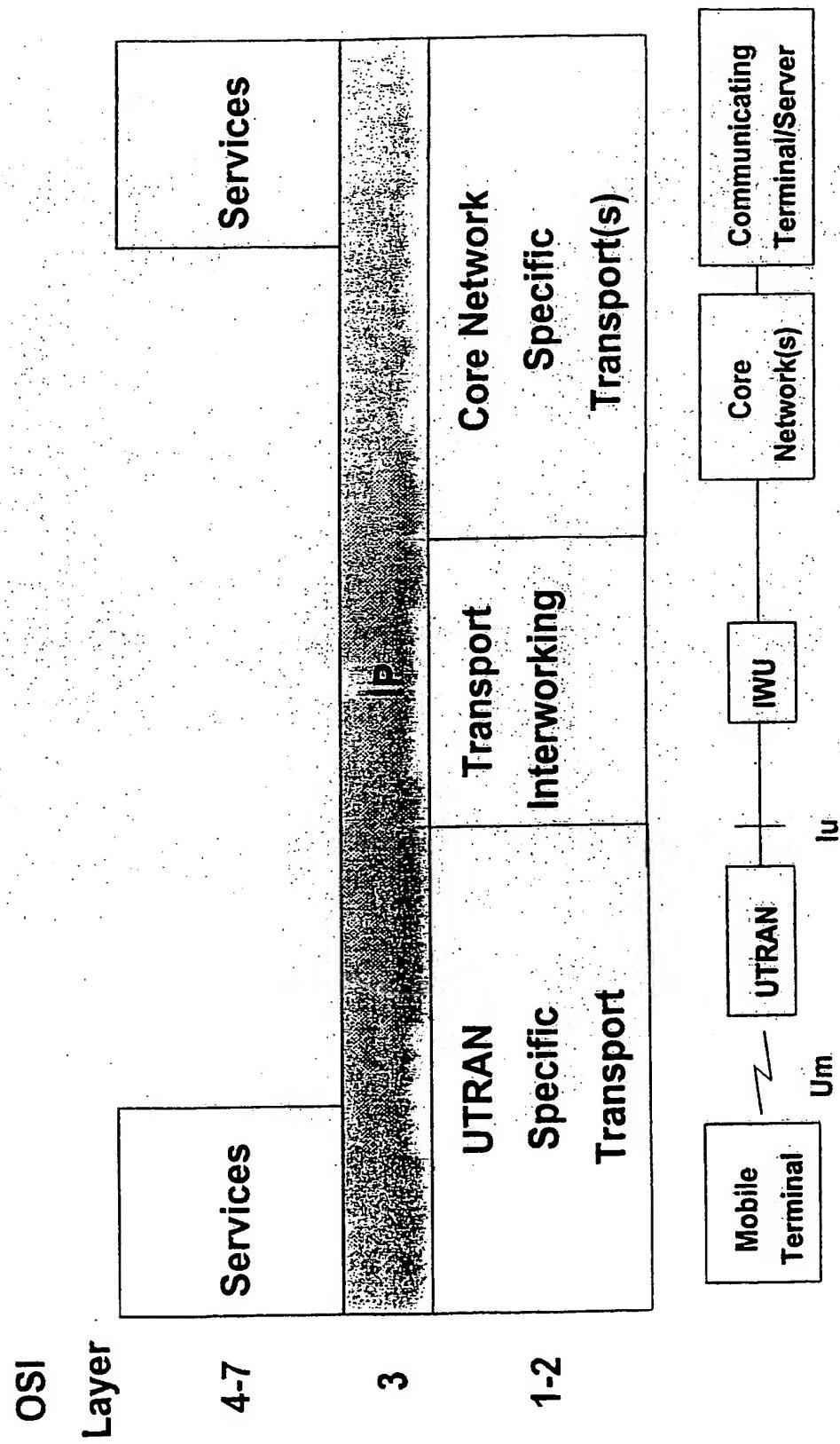
FIGURE 4

FIGURE 5

6/8
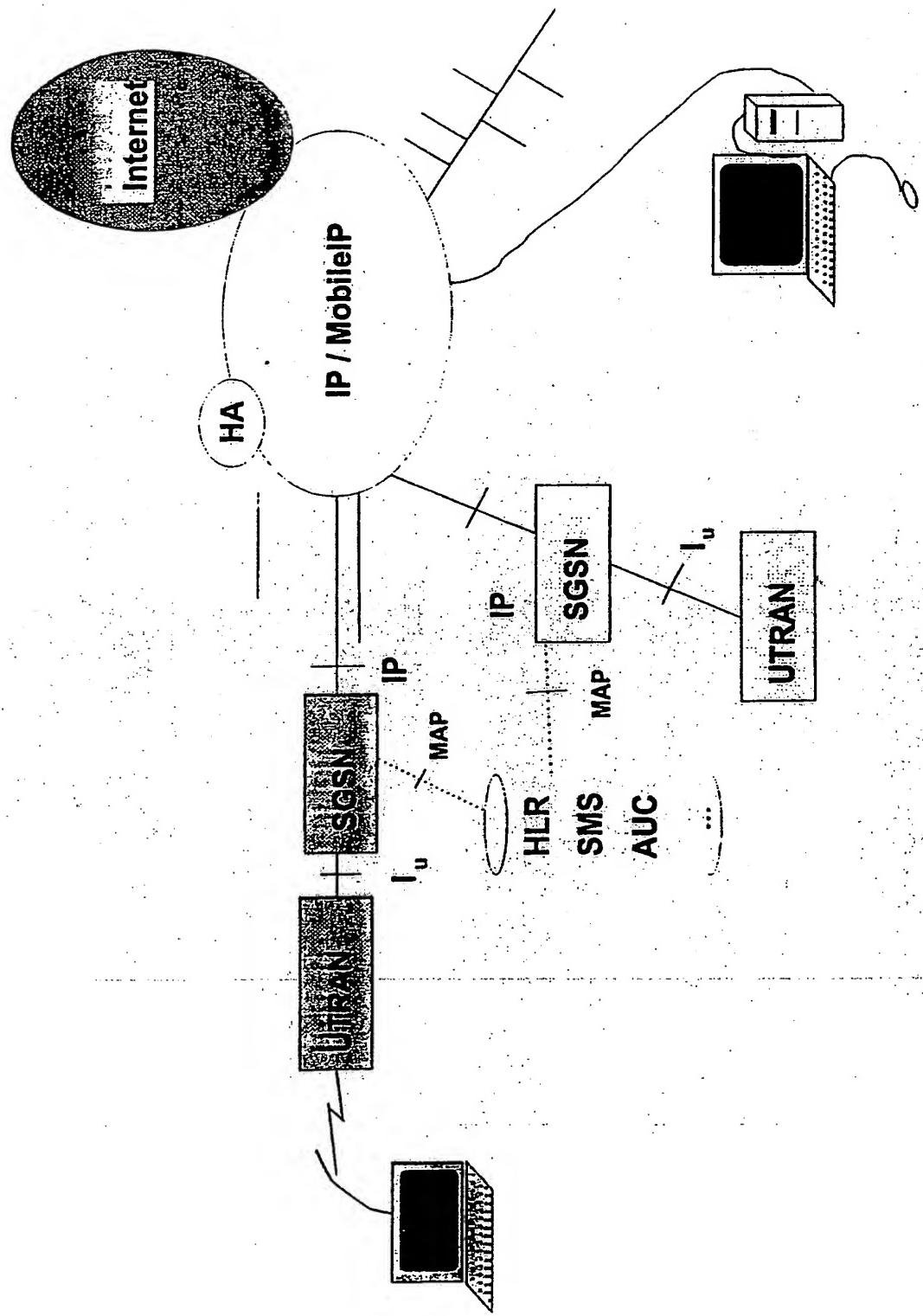


FIGURE 6

— Data & Signalling

......... Signaling

FIGURE 7

Internet

IP / MobileIP foreign network

IP / MobileIP home network

HA

HA

SGSN

SGSN

SGSN

SGSN

UTRAN

UTRAN

UTRAN

IP

IP

IP

$I_u$

$I_u$

$I_u$

MAP / SS7

MAP

MAP

HLR
SMS
AUC

——— Data & Signalling

·········· Signaling

FIGURE 8